UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,385	10/05/2001	Erik Riedel	10014506-1	5125

7590 05/12/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ABYANEH, ALI S	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 05/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/972,385	**Applicant(s)** RIEDEL ET AL.
	Examiner Ali S. Abyaneh	**Art Unit** 2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 October 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on *05 October 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *10/05/2001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

4

DETAILED ACTION

1. Claims 1-35 are presented for examination.

Information Disclosure Statement PTO-1449

2. The Information Disclosure Statement submitted by applicant on 10/05/2001 has been considered. Please see attached PTO-1449.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-5,7-9,13-15,17,18,20,23,24 and 28-34 are rejected under 35 U.S.C. 102(e) as being anticipated by William J. Bolosky et al. (US Publication NO.2002/0194484).

Regarding Claim 1

Bolosky teaches a method of file access control comprising: storing encrypted filename of a file at a location in a computing system (paragraph [0033] and [0034]);

converting the encrypted filename into a plaintext filename (paragraph [0156]);

modifying the plaintext filename into a modified filename (paragraph [0160]); and

authorizing an entity to access the file for performing a type of operation on the file based on the modified filename (paragraph [0119]).

Regarding Claims 2and 17

Bolosky teach all limitation of the claim as applied to claim 1 and 15 above and furthermore he teaches a method/apparatus, wherein said converting comprises using a combination of two encryption keys to convert the encrypted filename into the plaintext filename (paragraph [0154]-[0156]).

Regarding Claims 3, 18 and 20

Bolosky teach all limitation of the claim as applied to claim 2 and 17 above and furthermore he teaches a method, wherein said modifying comprises using a first one of the two encryption keys to encrypt the plaintext filename into the modified filename and using a first one of the two encryption keys to encrypt the plaintext filename (paragraph [0119] (randomly generated key K)).

Regarding Claim 4

Bolosky teaches all limitation of the claim as applied to claim 3 above and furthermore he teaches a method, wherein said authorizing comprises using the second one of the two encryption keys to encrypt the modified filename to form a result and determining whether the result matches the encrypted filename (paragraph [0154]-[0156]).

Regarding Claim 5

Bolosky teaches all limitation of the claim as applied to claim 2 above and furthermore he teaches a method, wherein said modifying comprises using a first one of the two encryption keys to encrypt the plaintext filename and performing a hash function on the filename thereby forming the modified filename (paragraph [0037]).

Regarding Claim 7

Bolosky teaches all limitation of the claim as applied to claim 1 above and furthermore he teaches a method, wherein said encrypted filename is encrypted using a first key prior to said storing and further comprising storing a second encrypted filename of the file at the location wherein the second encrypted filename is encrypted using a second key prior to said storing (paragraph [0037][0038]).

Regarding Claim 8

Bolosky teaches all limitation of the claim as applied to claim 7 above and furthermore he teaches a method, wherein said converting comprises using the first key to convert the encrypted filename into the plaintext filename (paragraph [00154]).

Regarding Claim 9

Bolosky teaches all limitation of the claim as applied to claim 8 above and furthermore he teaches a method, wherein said modifying comprises using the second key to encrypt the plaintext filename into the modified filename (paragraph [0119]).

Regarding Claims 13 and 14

Bolosky teaches all limitation of the claim as applied to claim 1 above and furthermore he teaches a method, wherein said storing comprises substituting said encrypted filename into a directory structure at the location in place of the plaintext filename and encrypting the data of the file (paragraph [0033]).

Regarding Claim 15

Bolosky teaches an apparatus for controlling access to a filename, comprising: a server for the storing an encrypted file and a client in communication with the server for retrieving the encrypted filename from the server (paragraph [0031], [0033] and [0034]), for converting the encrypted filename into a plaintext filename (paragraph [0156]) and for modifying the plaintext filename into a modified filename (paragraph [0160]); wherein the client provides the modified filename to the server and wherein the server determines whether the client is authorized to perform a type of operation on the file based on the modified filename received from the client (paragraph [0119]).

Regarding Claim 23

Bolosky teaches all limitation of the claim as applied to claim 15 above and furthermore he teaches an apparatus, wherein the encrypted filename is encrypted using a first key and wherein the server stores a second encrypted filename and the second encrypted filename is encrypted using a second key (paragraph [0037][0038]).

Regarding Claim 24

Bolosky teaches all limitation of the claim as applied to claim 23 above and furthermore he teaches an apparatus, wherein the client converts the encrypted filename into the plaintext filename using the first key and modifies the plaintext filename into the modified filename using the second key (paragraph [0119].

Regarding Claim 28

Bolosky teaches an apparatus for controlling access to a file comprising a server having a stored encrypted filename of a file (paragraph [0031], [0033] and [0034] (examiner considers distributed file system as applicant's server)), the server being in communication with a writer and a reader, the writer being a client of the server and having a first key that permits the writer to write to the file and the reader being another client of the server and having a combination of the first key and a second key wherein the combination permits the reader to read the file. (paragraph [0119] (examiner considers one of the user in Bolosky multiple user system as applicant's writer client and any other user in Bolosky multiple user system as applicant's reader client of the server.

Randomly generated key (K) that corresponds to applicant's first key is being used to write the file and combination of K and public key that corresponds to applicant's combination of first and second key is being used to read the file)).

Regarding Claim 29

Bolosky teaches all limitation of the claim as applied to claim 28 above and furthermore he teaches an apparatus, wherein the stored encrypted filename is obtained by encrypting a filename of the file using the combination of the first key and the second key (paragraph [0119]).

Regarding Claim 30

Bolosky teaches all limitation of the claim as applied to claim 29 above and furthermore he teaches an apparatus, wherein the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, encrypting the received filename again using the second key thereby forming a twice encrypted filename and comparing the twice encrypted filename to the stored encrypted filename. (paragraph [0119]-[0130]).

Regarding Claim 31

Bolosky teaches all limitation of the claim as applied to claim 29 above and furthermore teaches an apparatus, wherein the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, applying a hash function to the received filename thereby forming a computed hash value and comparing the computed hash value to a stored hash value. (paragraph [0119]-[0130]).

Regarding Claim 32

Bolosky teaches an apparatus for controlling access to a file comprising a server having a first stored encrypted filename of the file and a second stored encrypted filename of the file (paragraph [0031], [0033] and [0034](examiner considers distributed file system as applicant's server and replicated copies of the files as applicant' second stored encrypted filename)), the server being in communication with a writer and a reader, the writer being a client of the server and having a first key that permits the writer to write to the file and the reader being another client of the server and having a second key that permits the reader to read the file (paragraph [0119] (examiner considers one of the user in Bolosky multiple user system as applicant's writer client and any other user in Bolosky multiple user system as applicant's reader client of the server . Randomly generated key (K) that corresponds to applicant's first key is being used to write the file and public key that corresponds to applicant's second key is being used to read the file)).

Regarding Claim 33

Bolosky teaches all limitation of the claim as applied to claim 32 above and furthermore he teaches an apparatus, wherein the reader decrypts the first stored encrypted filename using the first key (paragraph [0154]-[0156]).

Regarding Claim 34

Bolosky teaches all limitation of the claim as applied to claim 33 above and furthermore he teaches an apparatus, wherein the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the second key and comparing the received filename to the second stored encrypted filename (paragraph [0119]-[0130]).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 6, 10, 11, 19, 21, 22, 25-27, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over William J. Bolosky et al. (US Publication NO.2002/0194484) in view of Edward A. Hubbard et al. (US Patent NO.6, 847,995).

Regarding Claims 6 and 10

Bolosky teaches all limitation of the claim as applied to claim 5 and 9 above but he does not explicitly teach, **wherein said authorizing comprises comparing the modified filename to a stored hash value and comparing the modified filename to the second encrypted filename**. However in an analogous art Hubbard teaches a method of comparing the modified file to stored hash value for authorization and comparing the modified file to the second encrypted file (column 39, lines 64-67 and column 40, lines 56-67). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bolodky to include comparing the modified filename to stored hash value and second encrypted filename. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order for the server system to determine a pass/fail response and provide an indication of the result of the hash check evaluation back to the client (column 40, lines 6-9).

Regarding Claim 11

Bolosky in view of Hubbard teach all limitation of the claim as applied to claim 10 above and he furthermore teaches a method, wherein said modifying further comprises performing a hash function on the filename after using the second key to encrypt the plaintext filename (paragraph [0037],[0073] and [0074]).

Regarding Claims 19 and 21

Bolosky teaches all limitation of the claim as applied to claim 18 and 20 above but he does not explicitly teach, **wherein said server determines whether the client is authorized to perform the type of operation on the file by using the second one of the two encryption keys to encrypt the modified filename to form a result and determines whether the result matches the encrypted filename provided by the**

client, and server performs a hash function on the filename form a result and determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value . However, in an analogous art Hubbard teaches a method wherein said server determines whether the client is authorized to perform the type of operation on the file by using the second one of the two encryption keys to encrypt the modified file to form a result and determines whether the result matches the encrypted file provided by the client, and server performs a hash function on the file form a result and determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value (column39, lines 56-67 and column 40, lines 1-35). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include server determines whether the client is authorized to perform the type of operation on the file by using the second one of the two encryption keys to encrypt the modified filename to form a result and determines whether the result matches the encrypted filename provided by the client, and server performs a hash function on the filename form a result and determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order for the server system to determine a pass/fail response and provide an indication of the result of the hash check evaluation back to the client (column 40, lines 6-9).

Regarding Claims 22 and 25

Bolosky teaches all limitation of the claim as applied to claim 17 and 24 above and he furthermore teaches a method an apparatus, wherein said client forms the modified filename using a first one of the two encryption keys to encrypt the plaintext filename and performs a hash function on the filename to form a result (paragraph [0037] and [0038]). Bolosky does not explicitly disclose, **wherein the server determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value and by comparing the modified filename to the second encrypted filename**. However, in an analogous art Hubbard teaches a method wherein server determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value and the modified file to the second encrypted file (column39, lines 56-67 and column 40, lines 1-35). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include server determines whether the client is authorized to perform the type of operation on the file by comparing the result to a stored hash value and the modified file to the second encrypted file. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order for the server system to determine a pass/fail response and provide an indication of the result of the hash check evaluation back to the client (column 40, lines 6-9).

Regarding Claims 26 and 27

Bolosky and Hubbard teach all limitation of the claim as applied to claim 25 above and Hubbard further teaches the server performs a hash function on the file after the client uses the second key to modify the file and client performs a hash function on the filename after using the second key to modify the file. (column 39, lines 50-67 and column 40, lines 1-36).

Regarding claim 35

Bolosky teaches all limitation of the claim as applied to claim 33 above but he does not explicitly teach, **server performs a hash function on the received filename before comparing the received filename to the second stored encrypted filename** However, in an analogous art Hubbard teaches an apparatus, wherein server performs a hash function on the received file before comparing the received file to the second stored encrypted filename (column 39, lines 50-67 and column 40, lines 1-36). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include server performs a hash function on the received filename before comparing the received filename to the second stored encrypted filename. This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to generate a hash value and encrypt it and send the encrypted hash value to receiving devices so that the encrypted hash value may be decrypted and compared to reconstructed hash value (column 3, lines 58-66).

7. Claims 12 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over William J. Bolosky et al. (US Publication NO.2002/0194484) in view of Edward M. Scheidt et al. (US Publication NO.2002/0062451).

Regarding Claims 12 and 16

Bolosky teaches all limitation of the claim as applied to claim 1 and 15 above but he does not explicitly teach **plaintext filename permits read access to the file and wherein said type of operation is a write operation**. However, in an analogous art Scheidt teaches a method wherein plaintext file permits read access to the file and wherein said type of operation is a write operation (paragraph [0057]). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include plaintext file permits read access to the file and wherein said type of operation is a write operation. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access control in the system (paragraph [0065]).

References Cited, Not Used

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S.Patent No. 6,523,116

This reference relates to a personal information data storage and retrieval system.

2. U.S.Patent No. 6,301,660

This reference relates to a computer system having a protection mechanism for protecting the content of a file.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571)272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh A·A
Patent Examiner
Art Unit 2133
04/13/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100